

**中国矿业大学计算机科学与技术学院**

**2020-2021(2)本科生计算机网络实验报告**

实验内容 协议报文分析

指 标 点 5.2 占报告分比 25%

学生姓名 学 号

专业班级

学 院 计算机科学与技术学院

任课教师 杨东平

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **课程基础理论掌握程度** | 熟练 🞏 | 较熟练 🞏 | 一般 🞏 | 不熟练 🞏 |
| **综合知识应用能力** | 强 🞏 | 较强 🞏 | 一般 🞏 | 差 🞏 |
| **报告内容** | 完整 🞏 | 较完整 🞏 | 一般 🞏 | 不完整 🞏 |
| **报告格式** | 规范 🞏 | 较规范 🞏 | 一般 🞏 | 不规范 🞏 |
| **实验完成状况** | 好 🞏 | 较好 🞏 | 一般 🞏 | 差 🞏 |
| **工作量** | 饱满 🞏 | 适中 🞏 | 一般 🞏 | 欠缺 🞏 |
| **学习、工作态度** | 好 🞏 | 较好 🞏 | 一般 🞏 | 差 🞏 |
| **抄袭现象** | 无 🞏 | 有 🞏 姓名: | | |

综合成绩： 任课教师签字：

年 月 日

**实验编号：03**

**项目名称：**协议报文分析

**实验内容：**

(1) 运用抓包工具，分别获取不同互联网访问情形下的本机网卡数据包；过滤捕获和过滤显示不同条件的数据包。

(2) 运用抓包工具，分别对不同互联网访问情形下的数据包进行逐层分析，给出各层协议的主要参数及意义；要求分别获取WWW服务、Email服务、QQ通信和迅雷文件下载四种不同网络服务过程中的数据包。

(3) 运用抓包工具，连续获取面向连接的互联网访问情形下的本机网卡数据包；对连续获取的数据包找到执行面向连接过程的报文，给出实现面向连接过程（TCP三次握手）的详细分析。

**实验要求：**

(1) 通过拓扑结构探测，懂得跨网连接的概念，以及跨网连接必须的设备；

(2) 通过tracert命令应用，给出校园网连接互联网的接入网结构；

(3) 运用抓包工具，实时抓包，记录包状态变化；

(4) 给出不同应用情境下的不同层次数据包的分析结果。

(5) 透过Web服务访问，分析HTTP协议工作过程，总结HTTP协议特点；透过HTTP工作过程分析，获取TCP协议的工作过程，验证连接建立的三次握手过程，以及滑动窗口工作机制（选做）。

**预习要求：**

提前通过互联网或在实验室开始实验前登录实验管理服务器，点击预习链接，阅览或下载实验指导书——预习\网络协议\进阶-IP分组基本报文分析。

**操作与观察：**

正确按照实验指导书步骤操作，观察记录下操作结果。

**实验报告要求：**

(1) 按照实验要求，完成全部实验内容

(2) 在标准实验报告书上填写全部实验操作记录和观察结果

(3) 登录实验管理服务器，提交实验报告电子档。

**实验报告内容：**

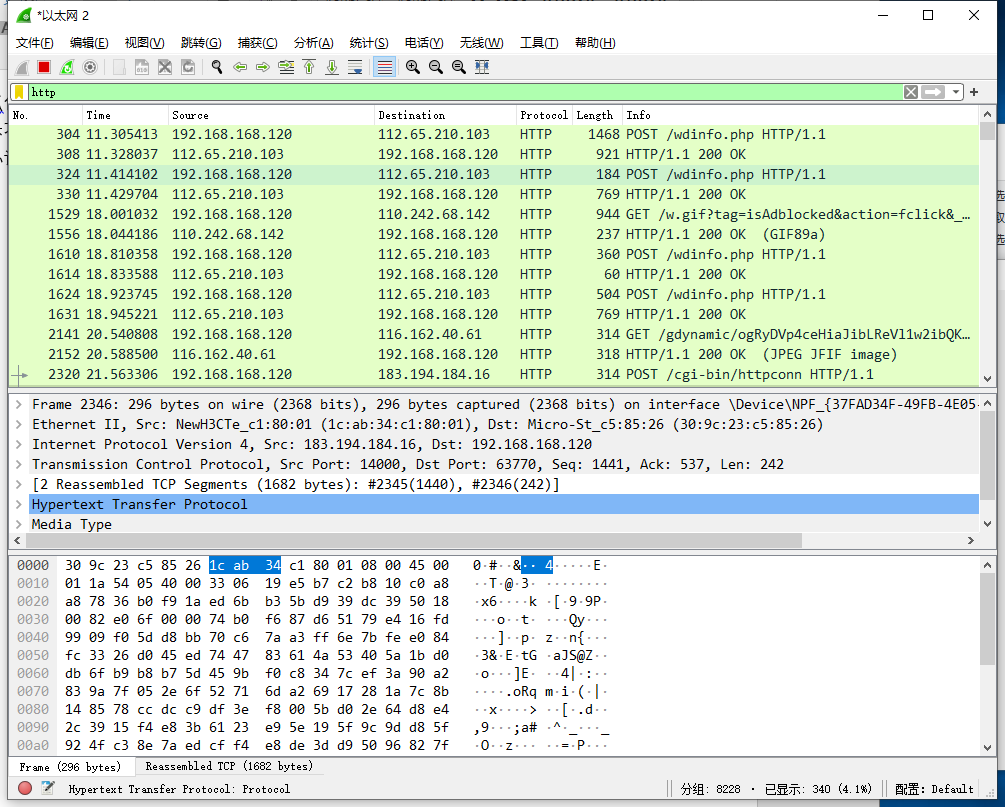
1. 运用抓包工具，分别获取不同互联网访问情形下的本机网卡数据包；过滤捕获和过滤显示不同条件的数据包。

图1.1 过滤HTTP协议

1. HTTP协议

通过过滤器找到了HTTP协议的数据包。

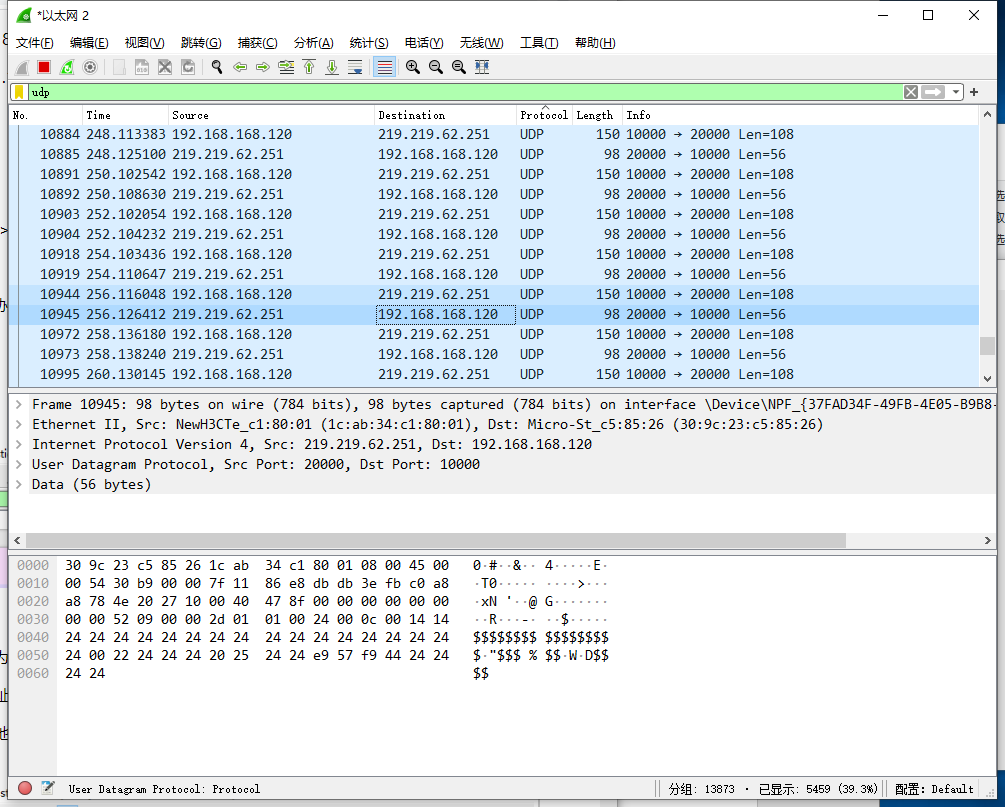
1. UDP协议

图1.2 过滤UDP协议

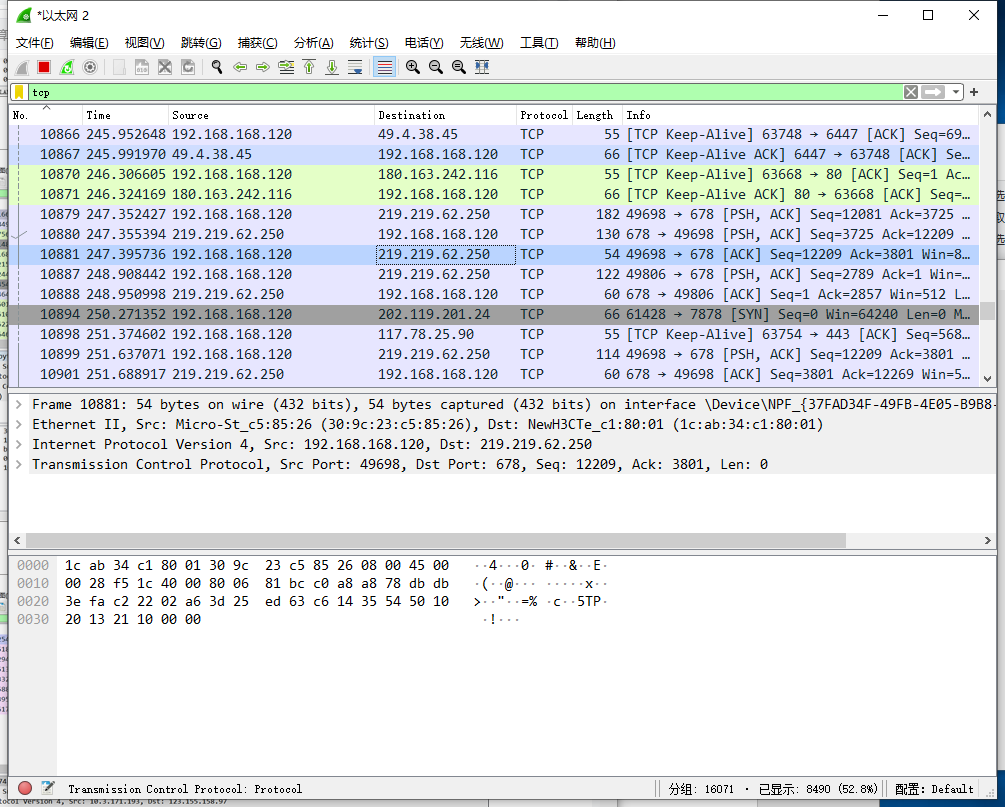
1. TCP协议

图1.3 过滤TCP协议

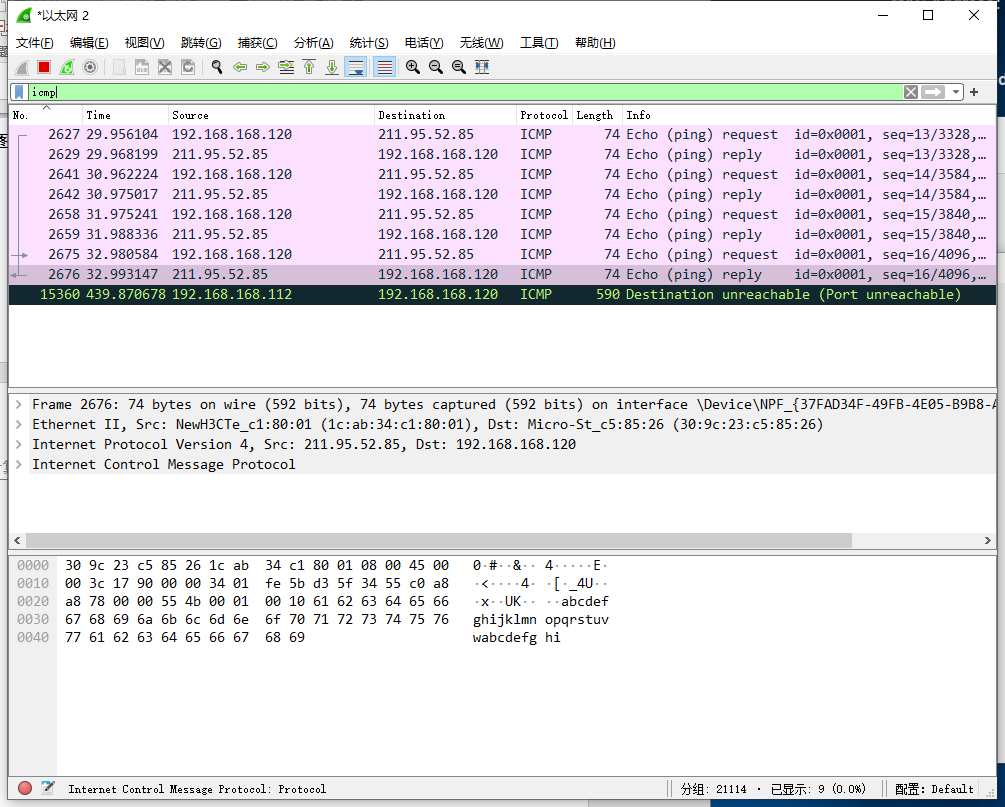
1. ICMP协议

图1.4 ICMP协议

总的来说，通过wireshark的过滤器的特定语法，可以过滤出想要的数据包。

1. 运用抓包工具，分别对不同互联网访问情形下的数据包进行逐层分析，给出各层协议的主要参数及意义；要求分别获取WWW服务、Email服务、QQ通信和迅雷文件下载四种不同网络服务过程中的数据包。
2. WWW服务的数据包抓取及分析

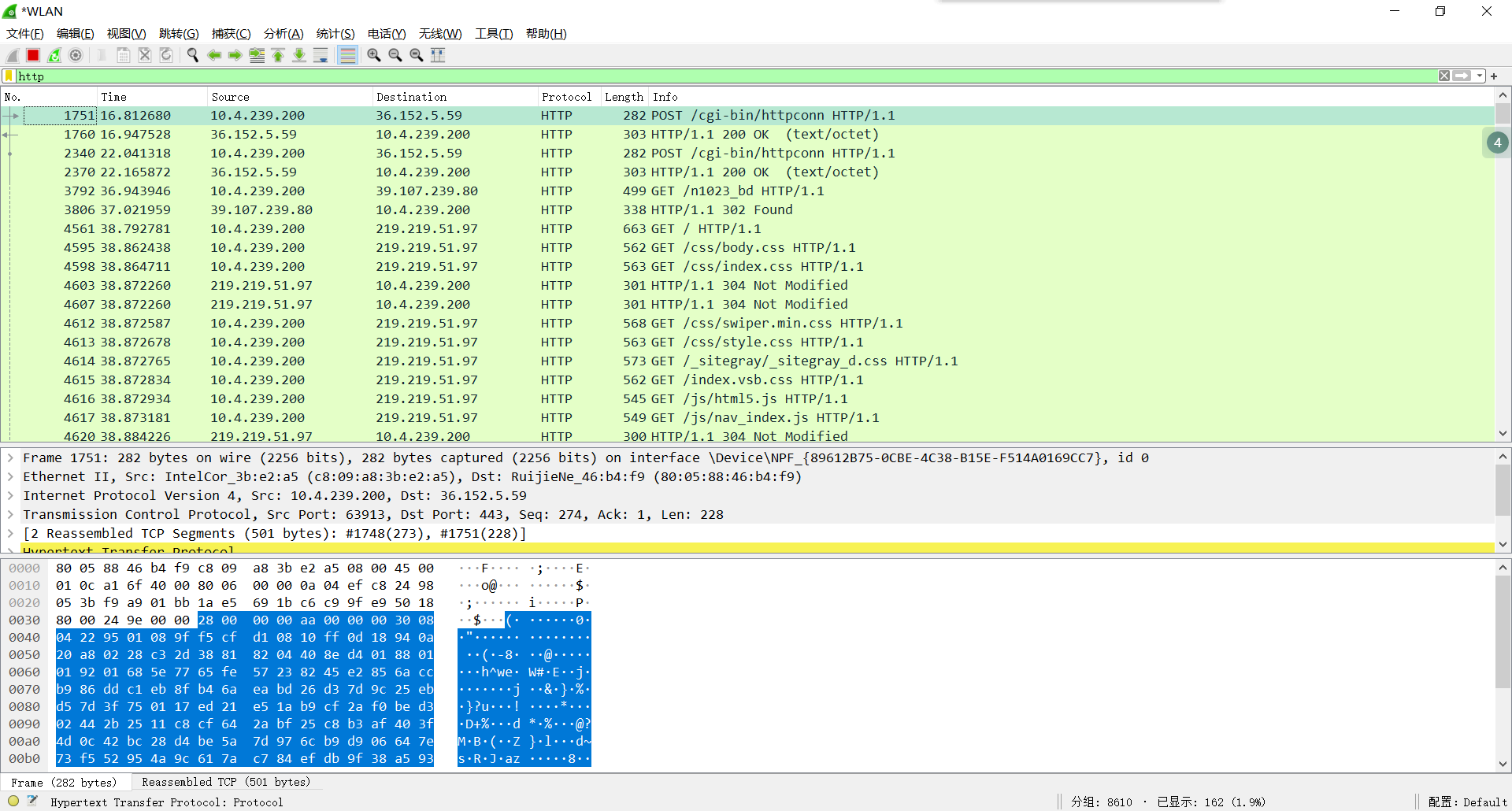
过滤出http数据报如图2.1.1所示

图2.1.1 抓取http数据报

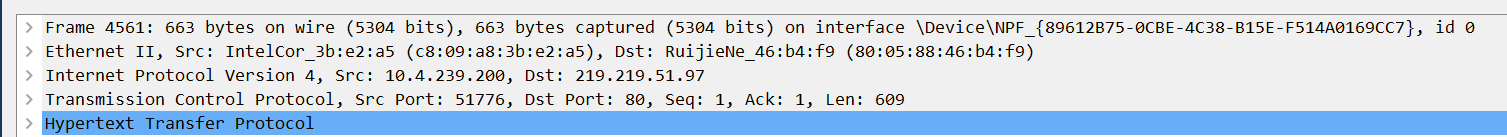
选择其中一个数据包分析，发现http数据包中有应用层、运输层、网络层、数据链路层以及物理层五层协议。如图2.1.2所示：

图2.1.2 五层协议

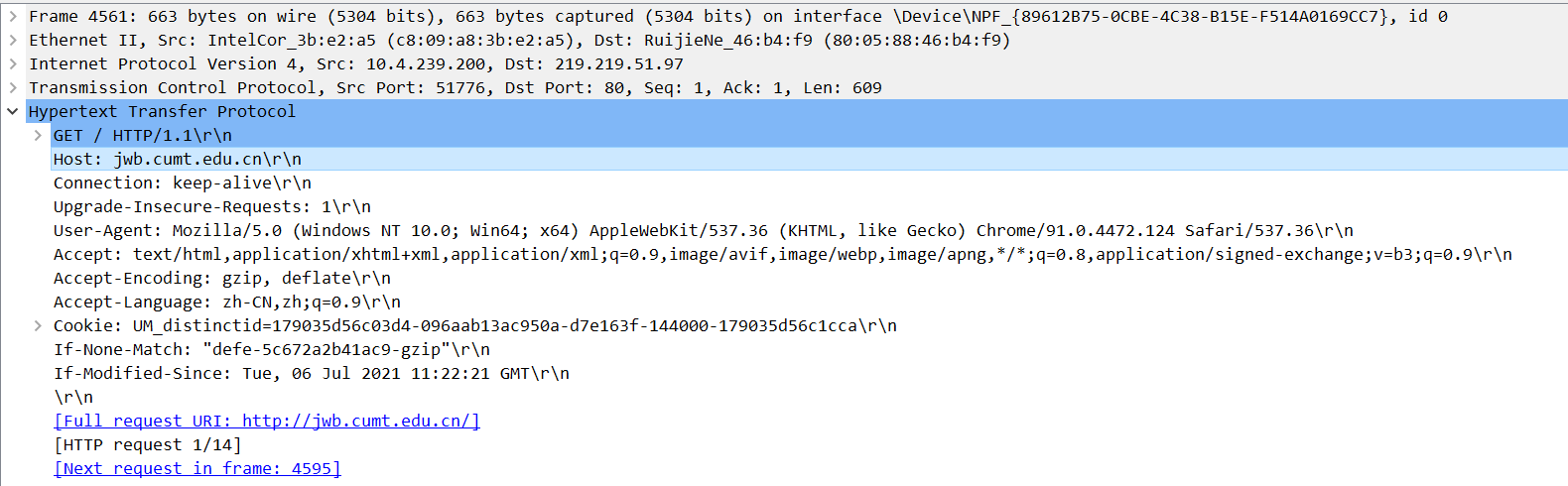
自上而下分析。应用层使用了超文本传输协议（hypertext transfer protocol），可以看出以GET方式请求数据，访问的主机为jwb.cumt.edu.cn，同时还携带了User-Agent，Cookie等一些请求头信息，如图2.1.3所示。

图2.1.3 应用层的信息

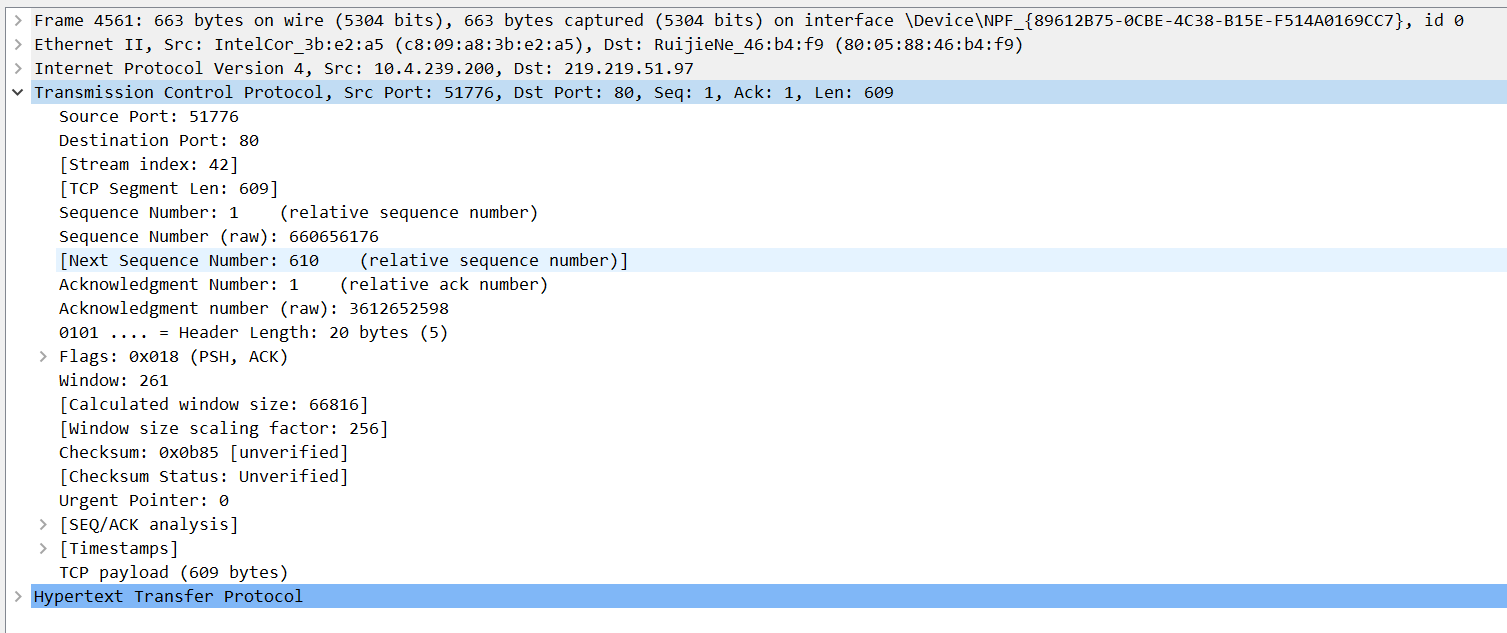
接下来分析运输层。运输层使用了TCP协议，可以看出源端口与目的端口分别是51776与80，Ack=1表示已经建立连接。还可以看除窗口（Window）值261、紧急指针（Urgent Pointer）字段为0等其他信息。如图2.1.4所示。

图2.1.4 传输层的信息

接下来分析网络层。网络层使用的是IPV4，可以看出源地址与目的地址分别是10.4.239.200，219.219.51.97，首部长度（Header Length）20字节，总长度（Total Length）649，生存时间TTL（Time To Live）128，还可以看出上层使用的是tcp协议（Protocol）等信息。如图2.1.5所示。

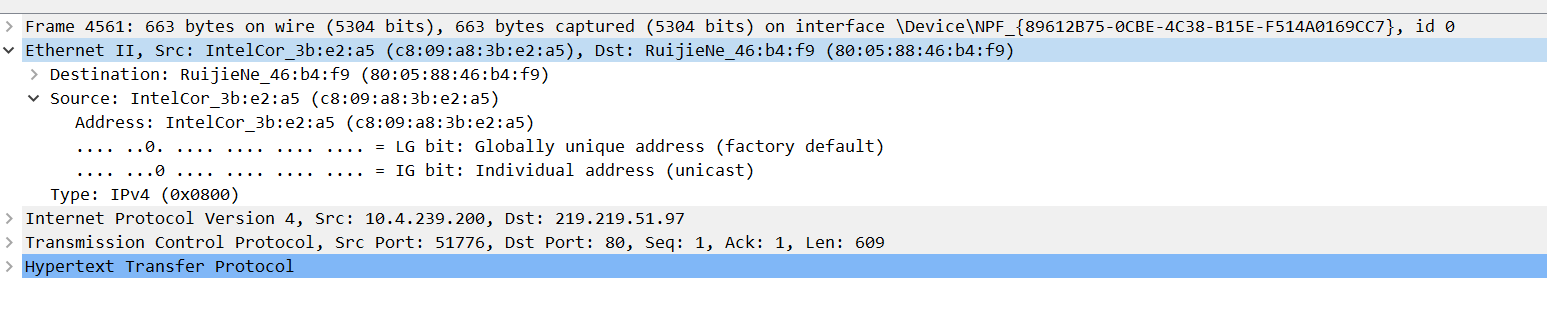
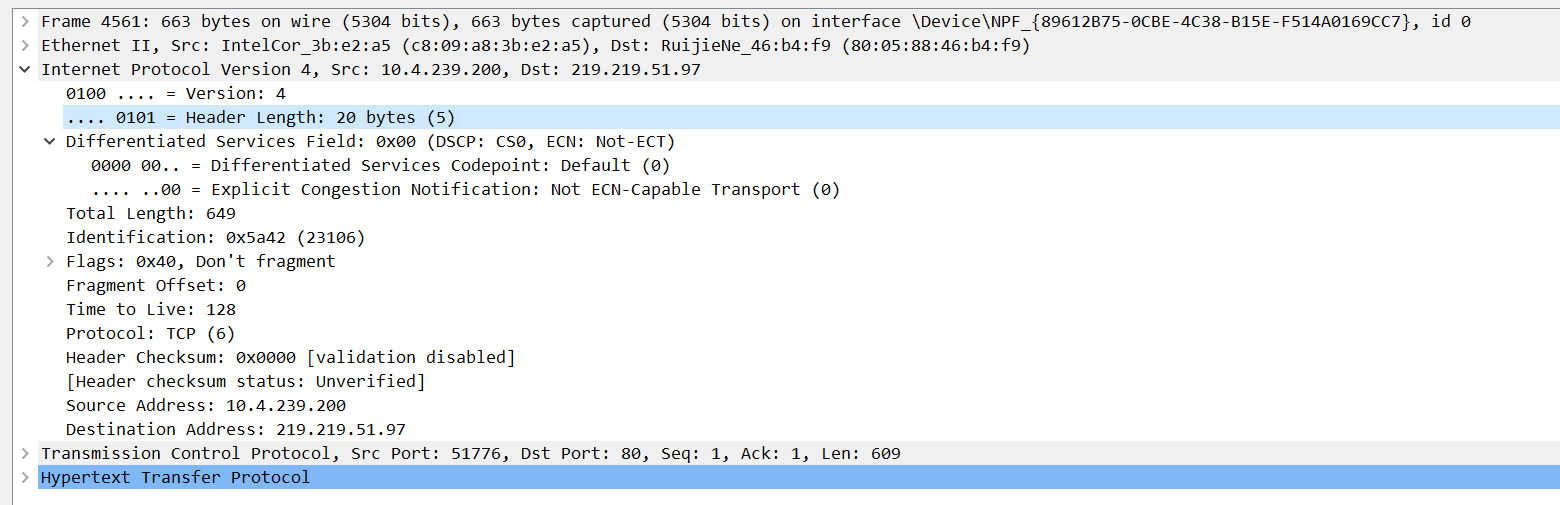
接下来分析数据链路层。可以看出源MAC地址以及目的MAC地址分别是c8-09-a8-3b-e2-a5、80-05-88-46-b4-f9，在类型（Type）字段标识出了上层使用的是IPV4，如图2.1.6所示。.

图 2.1.6 数据链路层的信息

图2.1.5 网络层的信息

1. Email服务

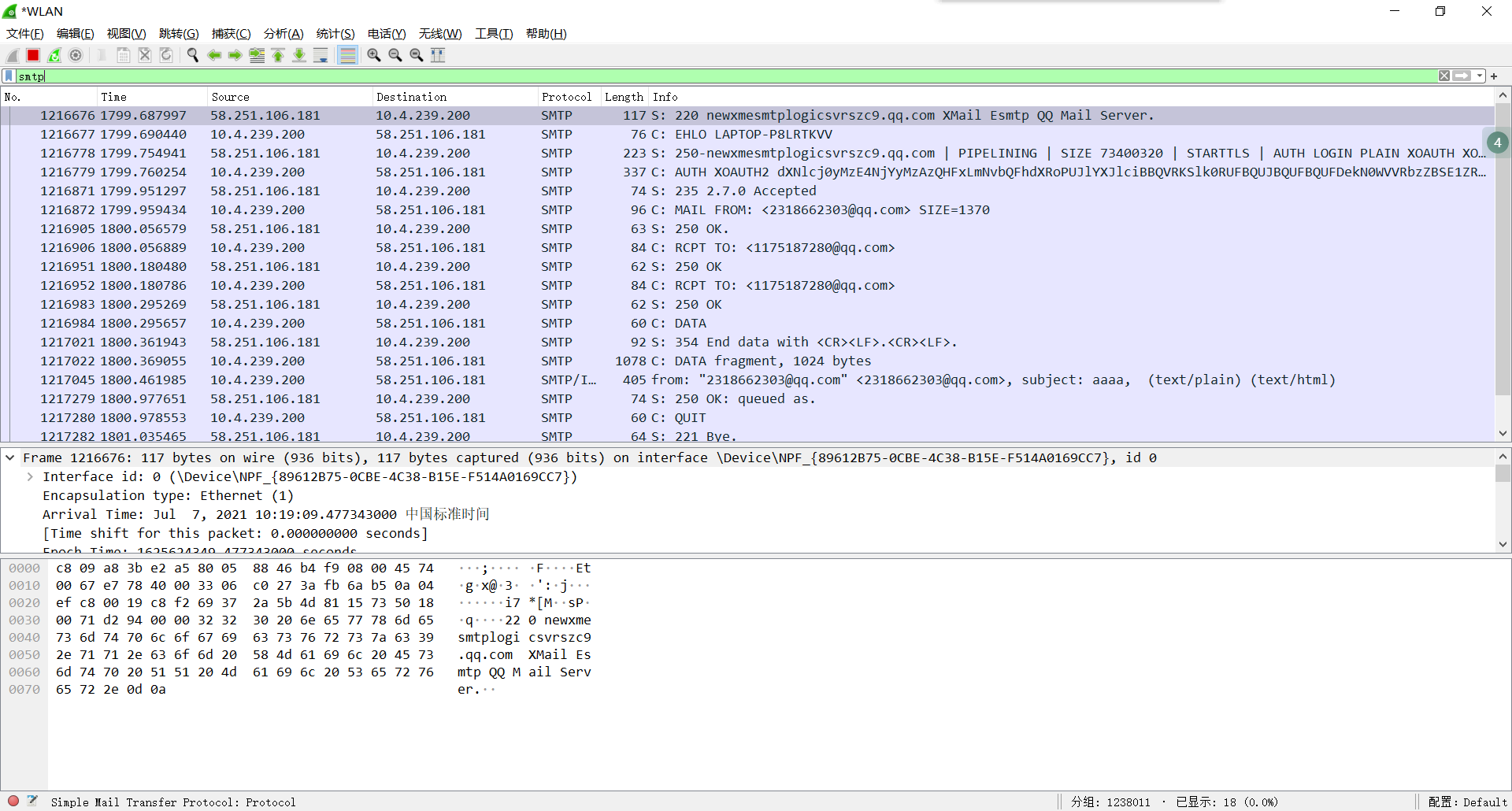
过滤出smtp协议的数据报如图2.2.1所示

图2.2.1 smtp协议

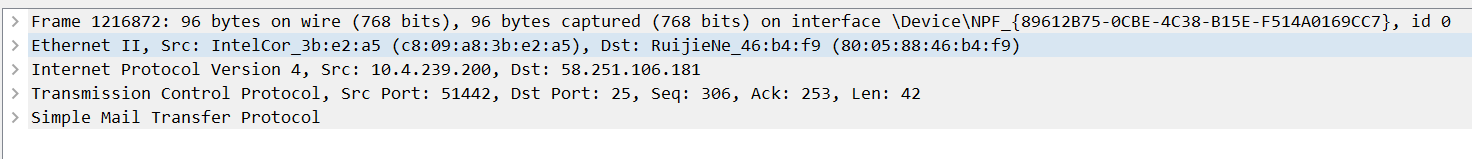
选择一个分组，发现使用的五层协议，其中应用层协议为SMTP（Simple Mail Transfer Protocol），如图2.2.2所示

图2.2.2 SMTP的五层协议

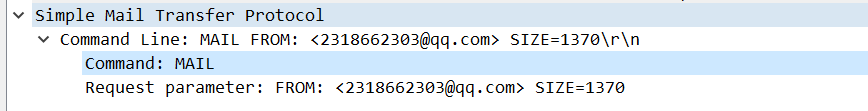
在应用层中，可以看出SMTP协议的接收参数是邮箱2318662303@qq.com.如图2.2.3所示。

图2.2.3 应用层信息

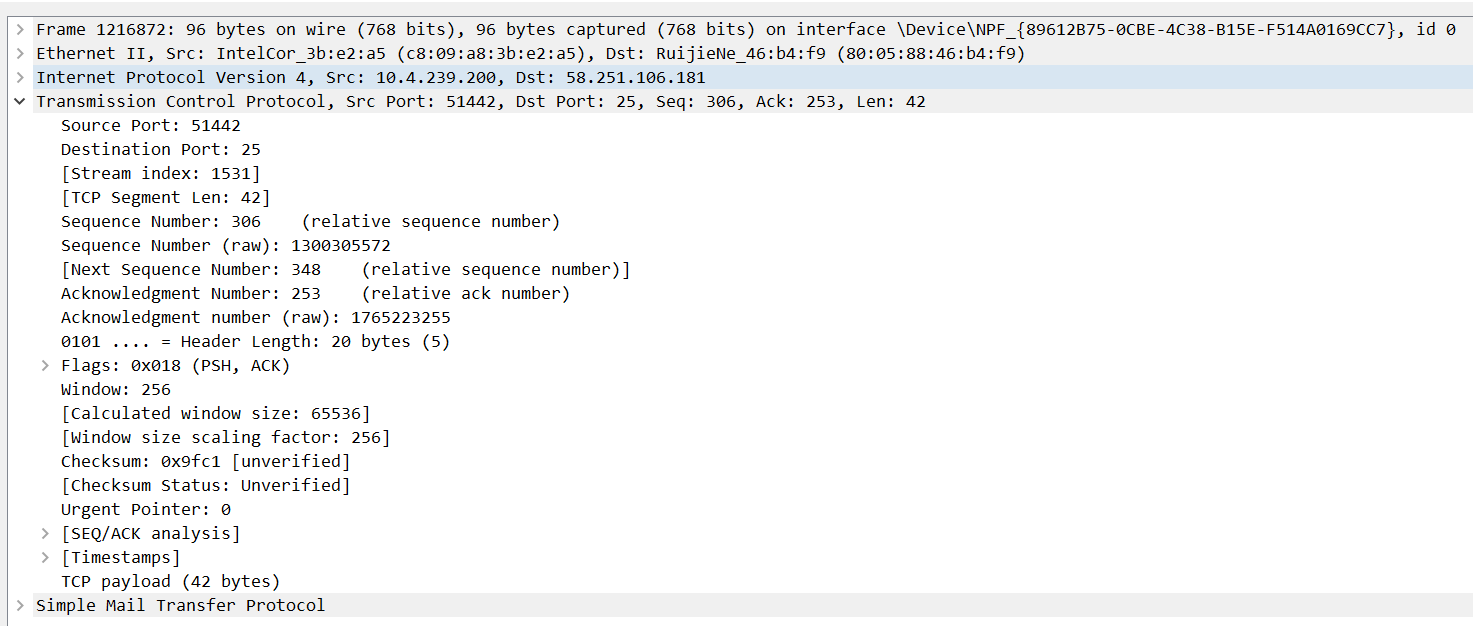
在运输层，同样可以看出源端口与目的端口分别是51442，25，窗口值256等TCP报文段的相关字段信息，如图2.2.4所示。

图2.2.4 运输层信息

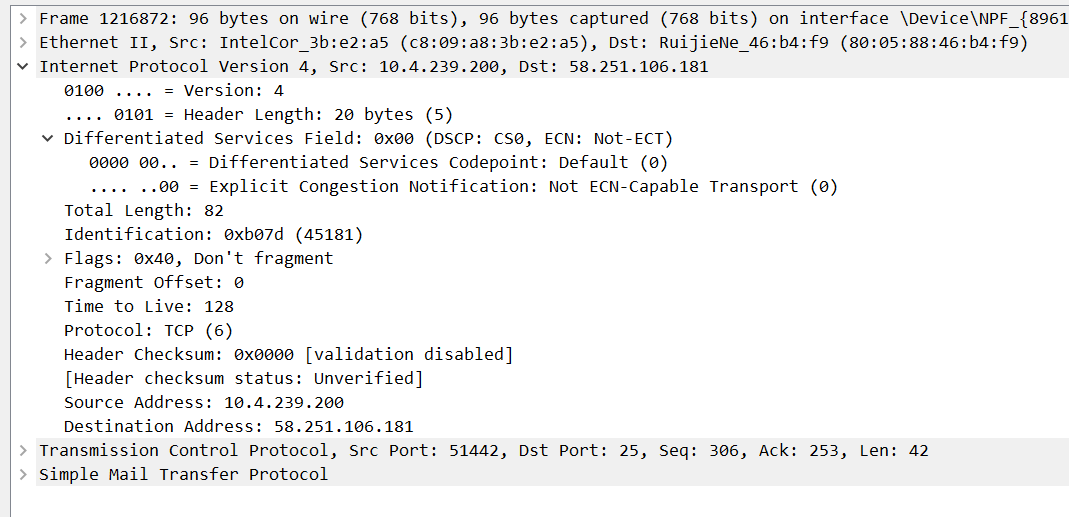
在网络层，可以看出源ip地址与目的ip地址分别是10.4.239.200、58.251.106.181，使用的是IPV4版本，生存时间128，上层是TCP协议等信息。如图2.2.5所示。

图2.2.5 网络层信息

数据链路层，同样可以看出源MAC地址与目的MAC地址分别是c8-09-a8-3b-e2-a5、80-05-88-46-b4-f9。可以看出数据部分封装的是IPV4数据报。如图2.2.6所示。

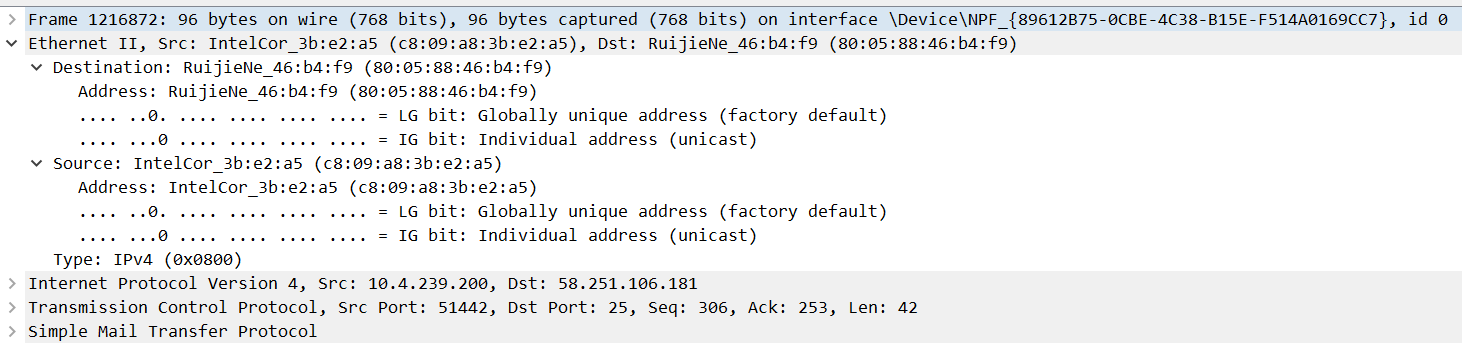
1. QQ通信

图2.2.6 数据链路层信息

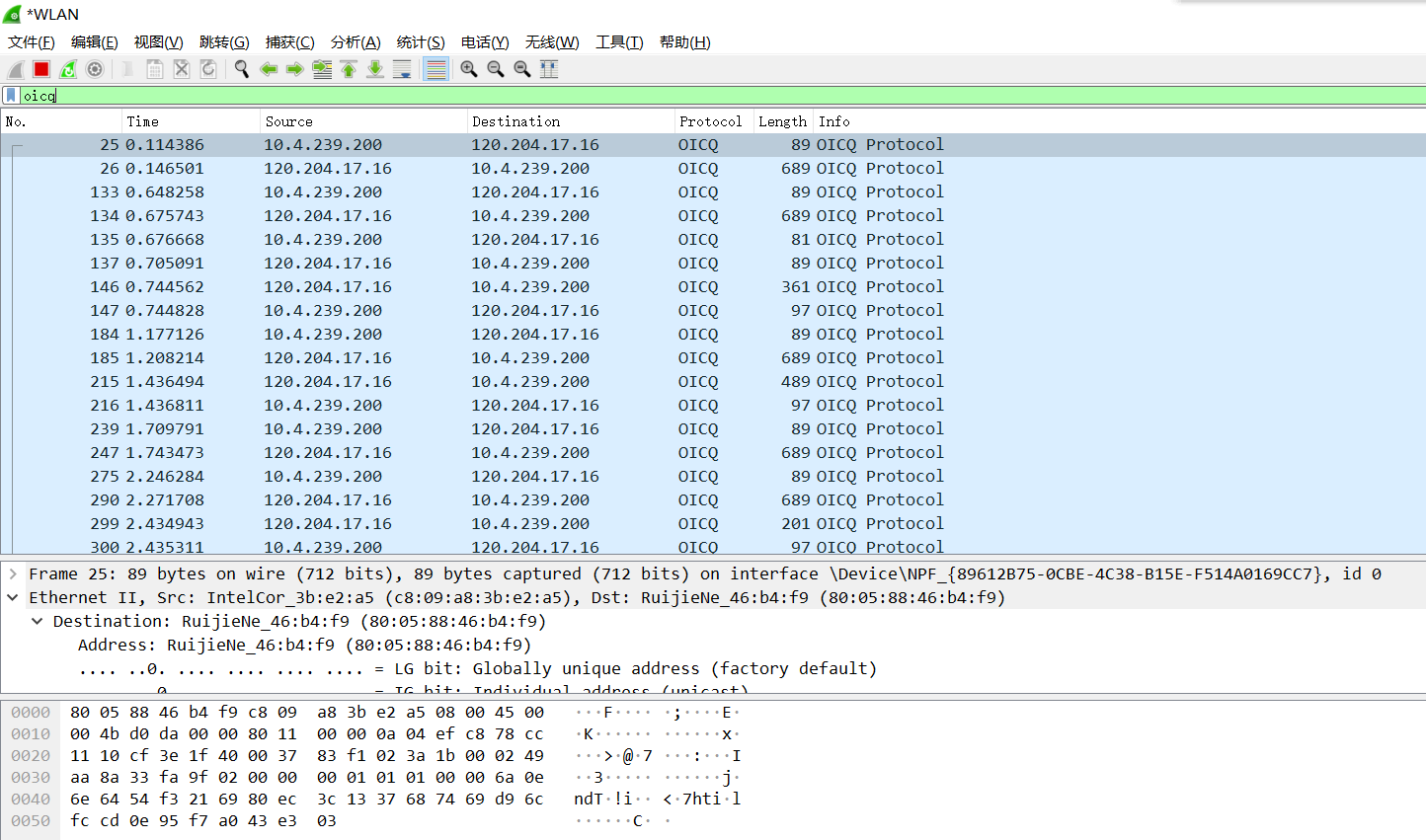
过滤出QQ通信所使用的OICQ协议的数据报，如图2.3.1所示。

图2.3.1 QQ通信的OICQ协议数据包

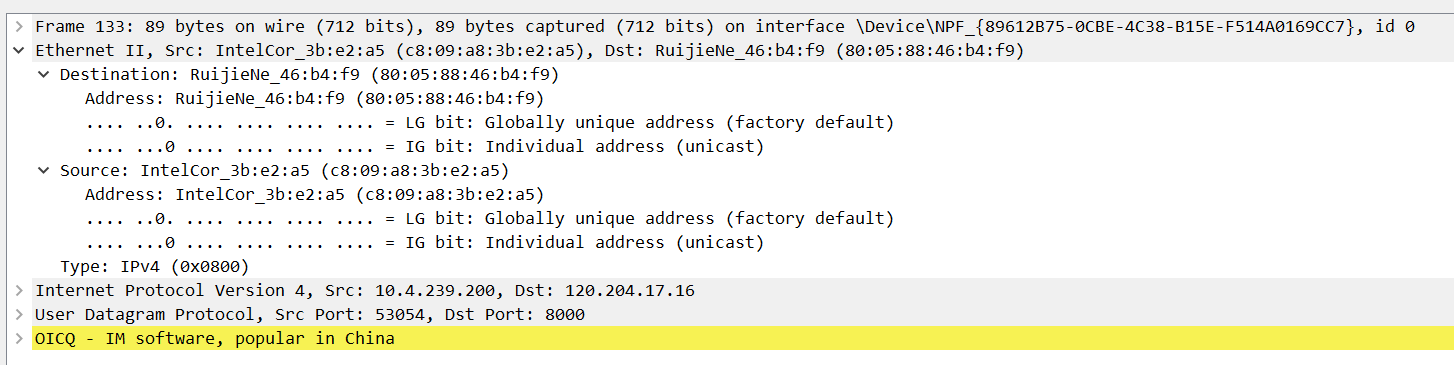
选择其中一个进行分析。可以看出，其应用层使用的是OICQ协议，如图2.3.2所示。

图2.3.2 应用层的OICQ协议

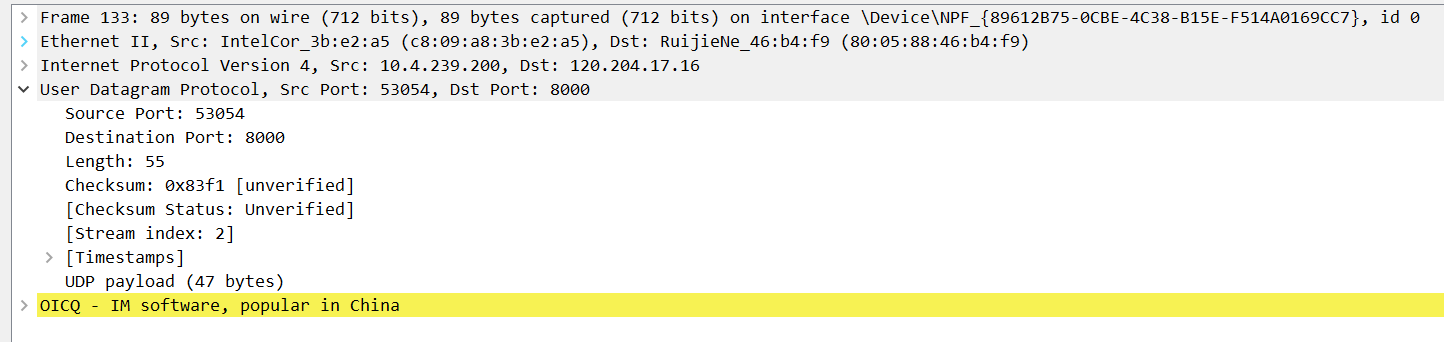
在运输层，使用的是UDP协议，可以看出源端口与目的端口号为53054与8000。UDP数据报的长度（Length）为55，如图2.3.3所示。

图2.3.3 运输层的UDP数据报

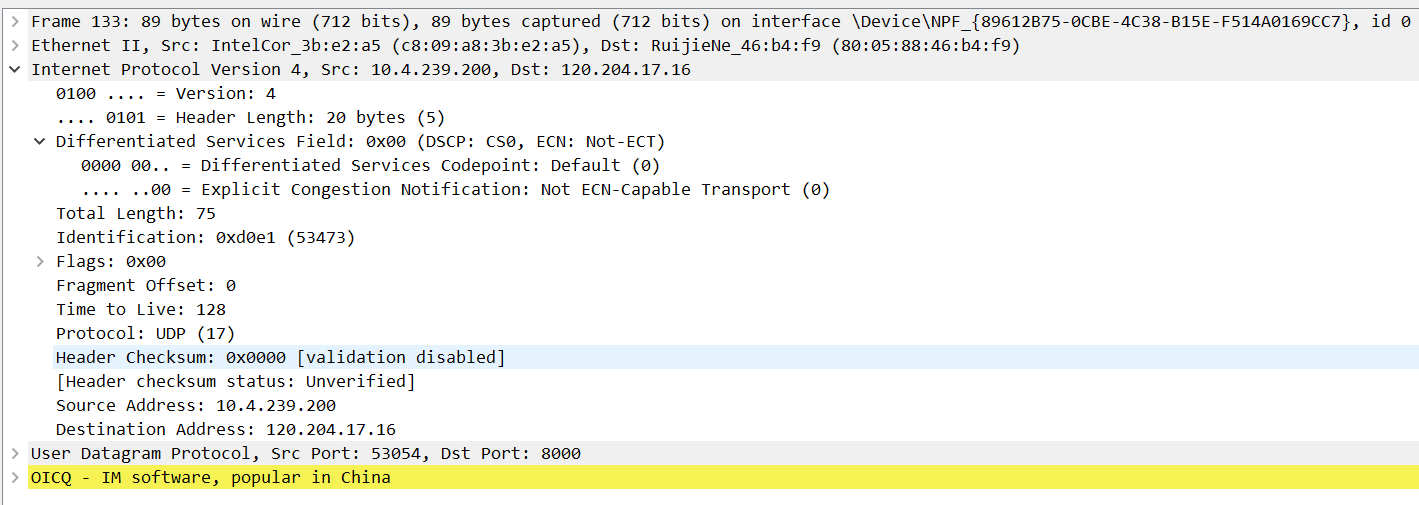
在网络层，除了可以看出源/目的IP地址等信息外，可以发现协议（Protocol）字段标明了上层协议使用的是UDP。如图2.3.4所示。

图2.3.4 网络层信息

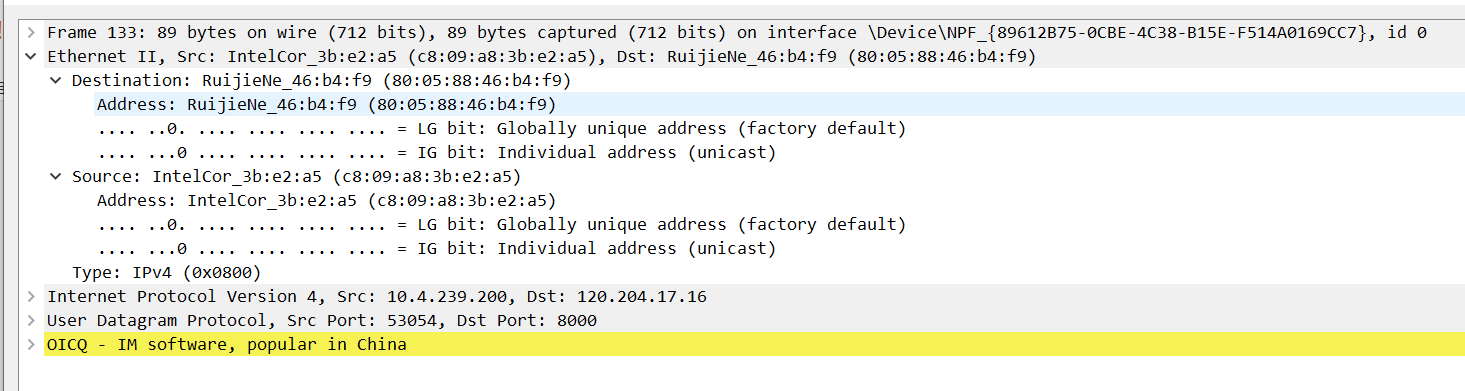
还有数据链路层的信息。表明上层是IPV4，源/目的MAC地址等信息。如图2.3.5所示。

图2.3.5 数据链路层信息

1. ICMP报文分析

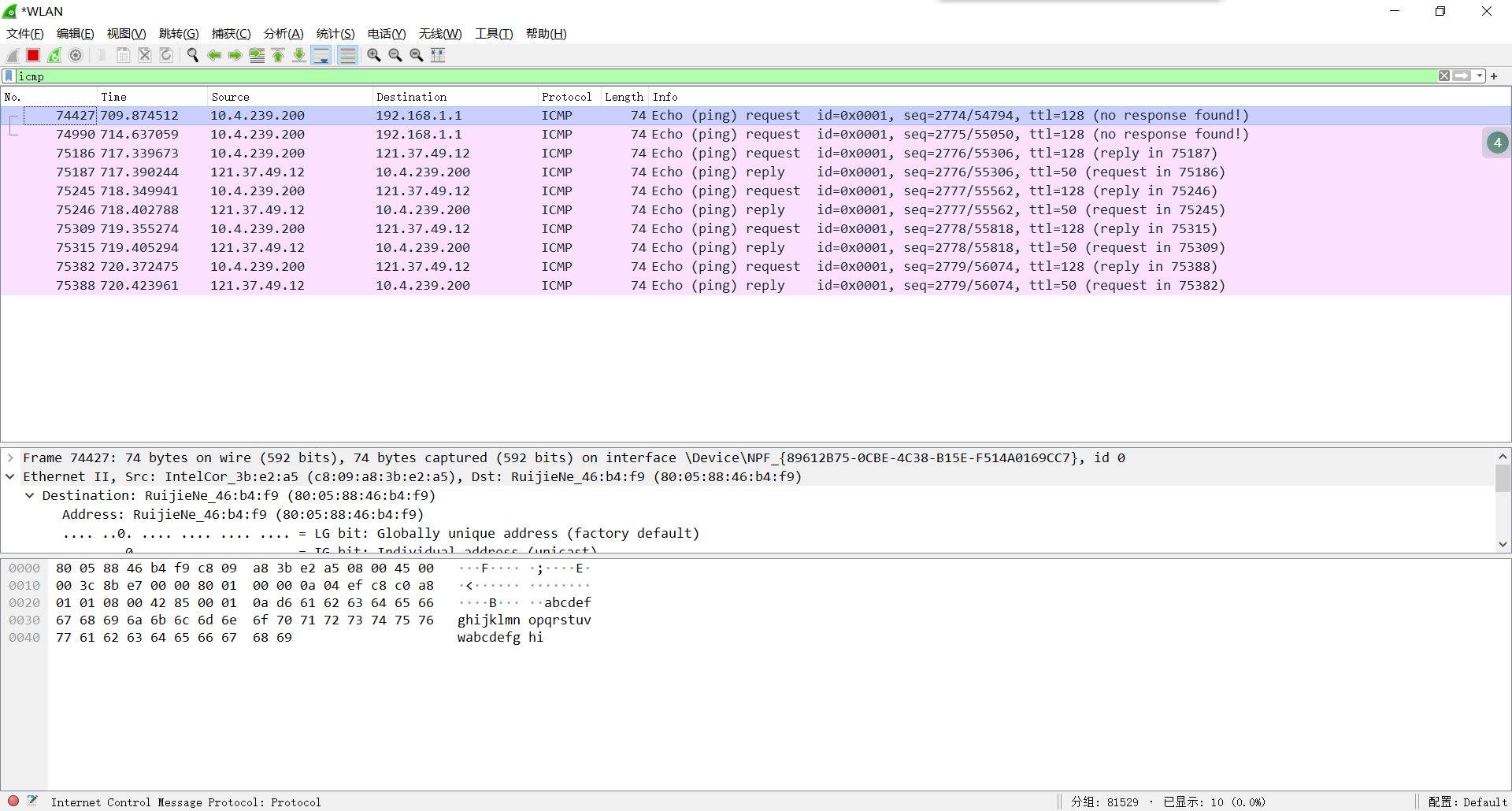
过滤到的ICMP报文如图2.4.1所示。使用了一次ping命令，于是捕获到了icmp报文。

图2.4.1过滤到的ICMP报文

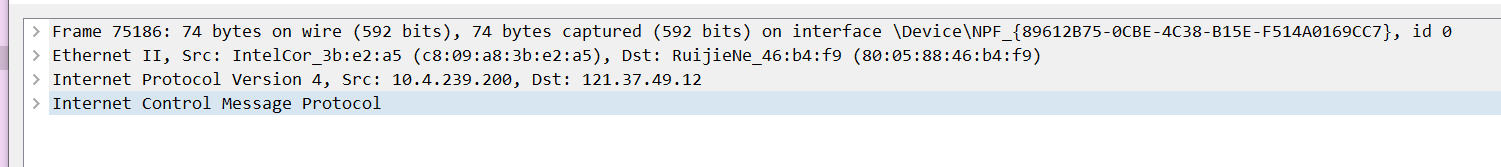
选取其中一个数据包，发现仅有物理层、数据链路层以及网络层信息。其中网络层的ICMP报文封装在了IP数据包的数据部分。如图2.4.2所示。

图2.4.2 ICMP数据报的层次

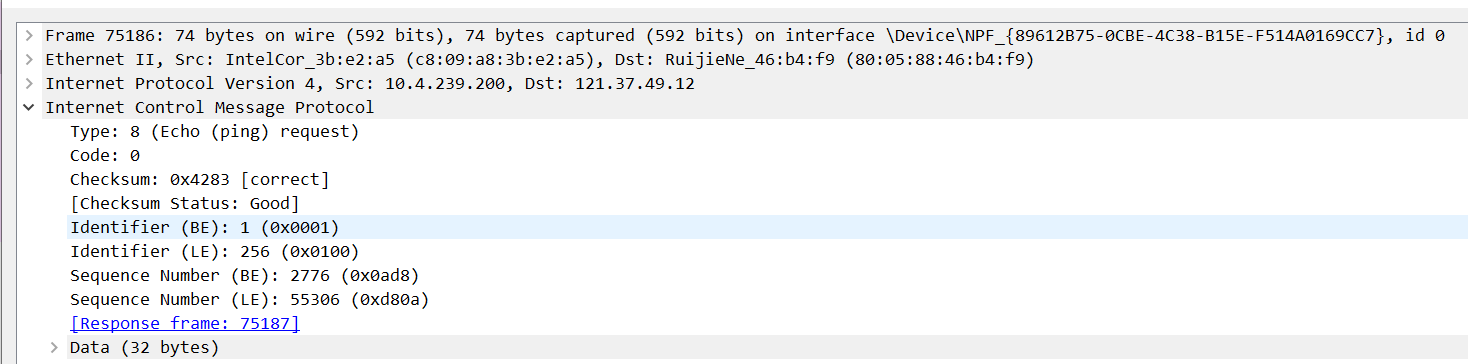
在ICMP报文中，可以看出ICMP的8字节首部与数据部分。其中首部中类型（Type）值为8，说明是一个ICMP询问报文，代码（Code）值为0，检验和（Checksum）值为0x4283H 等信息，如图2.4.3所示。

图2.4.3 ICMP报文的首部分析

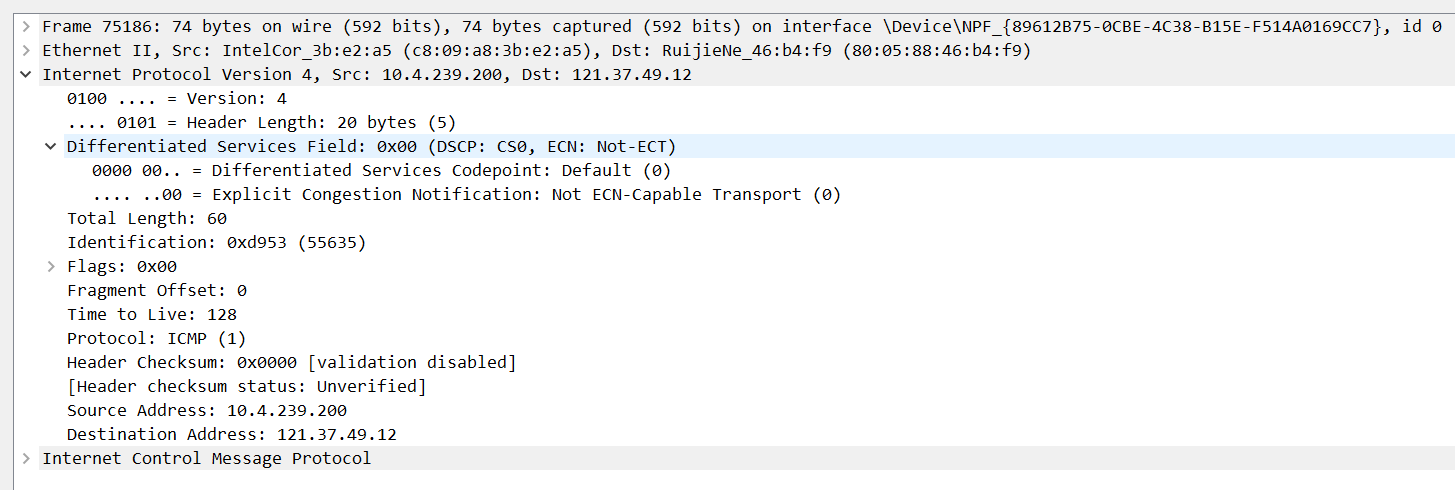
在IP层，可以看出源/目的ip地址分别是10.4.239.200、121.37.49.12，同时协议（Protocol）字段值为1，说明上层封装了ICMP报文，还有TTL=128等信息。如图2.4.4所示。

图2.4.4 网络层信息

同样，在数据链路层，可以看出上层使用的是IPV4，源/目的MAC地址分别是c8-09-a8-3b-e2-a5、80-05-88-46-b4-f9。如图2.4.5所示。

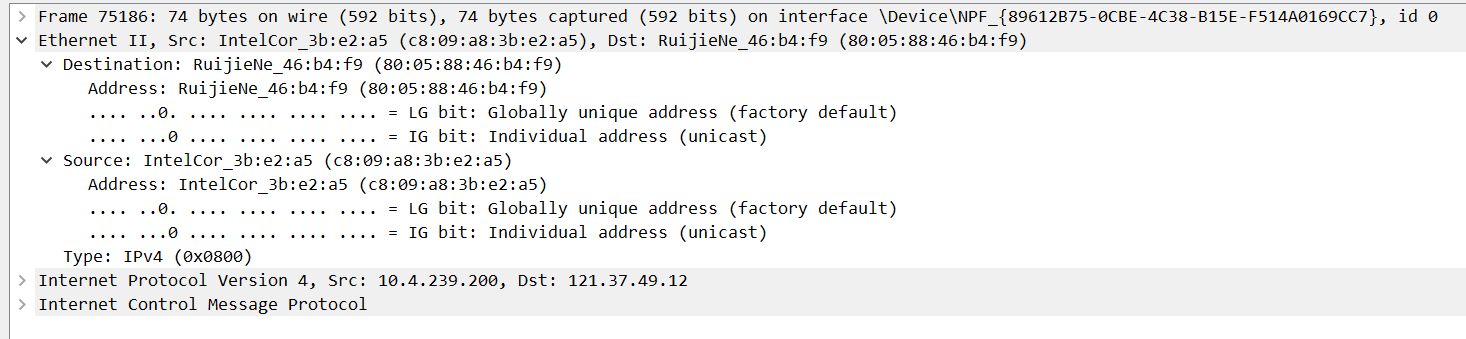


图2.4.5 数据链路层信息

1. 运用抓包工具，连续获取面向连接的互联网访问情形下的本机网卡数据包；对连续获取的数据包找到执行面向连接过程的报文，给出实现面向连接过程（TCP三次握手）的详细分析。

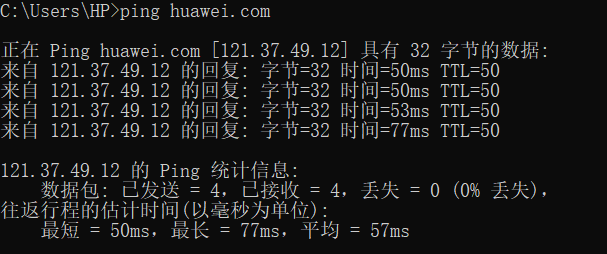
首先使用浏览器访问华为的官网huawei.com，建立连接。在命令行ping Huawei.com，得到访问的ip地址121.37.49.12，如图2.5.1所示。

图2.5.1 得到huawei.com的ip地址

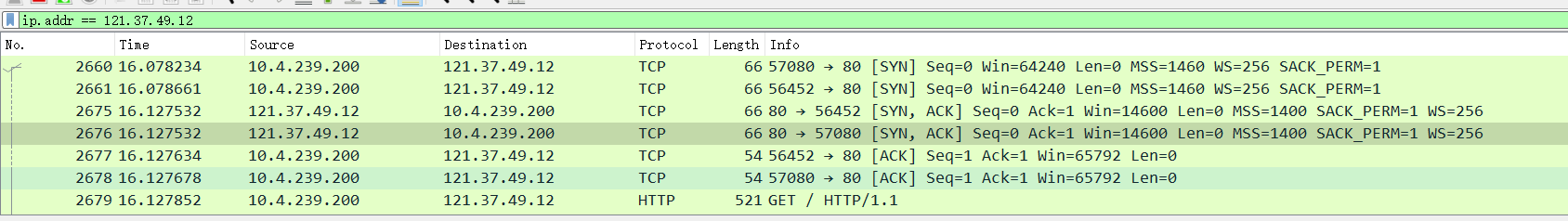
可以根据得到的ip地址在wireshark中过滤，结果如图2.5.2所示

图2.5.2 过滤得到TCP建立连接的数据包

在建立HTTP连接前发送了6个TCP数据报，即完成了两次三次握手过程。原因在info列中可以找到——分别建立了端口57080到端口80以及端口56452到端口80的连接，所以才有了“六次”握手的过程。下面仅分析端口80到端口57080的三次握手建立的过程：

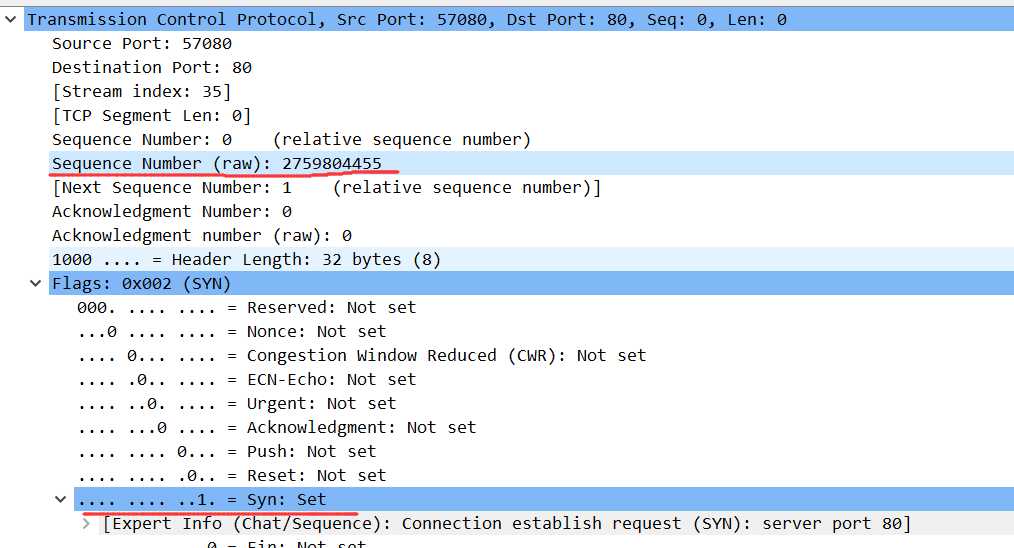
 首先，端口57080发送了第一次握手的TCP报文段，其中序列号seq=0xa47f4627（十进制2759804455），置SYN=1，如图2.5.3所示。

图2.5.3 第一次握手

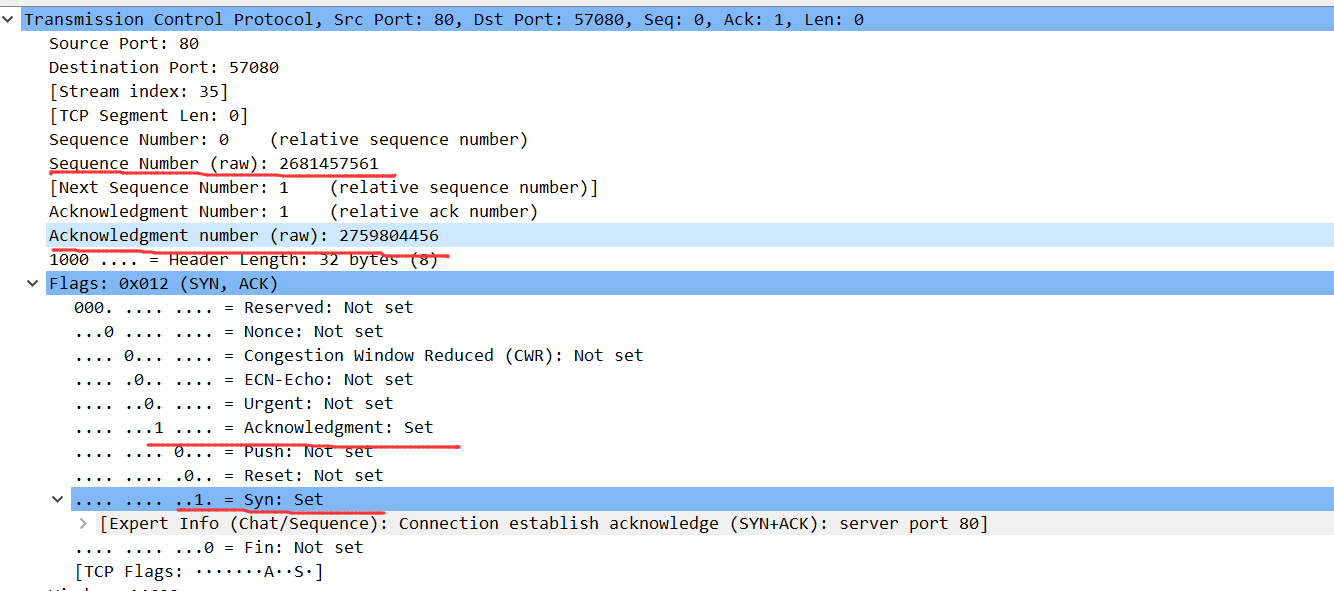
紧接着，端口80发送回了第二次握手的信息。可以看出，SYN=1，ACK=1，自身的序列号seq=0x9fd3cb99（十进制2681457561），确认号ack=0xa49f4628（十进制2759804456），确认号等于上一次的序列号+1。如图2.5.4所示。

图2.5.4 第二次握手

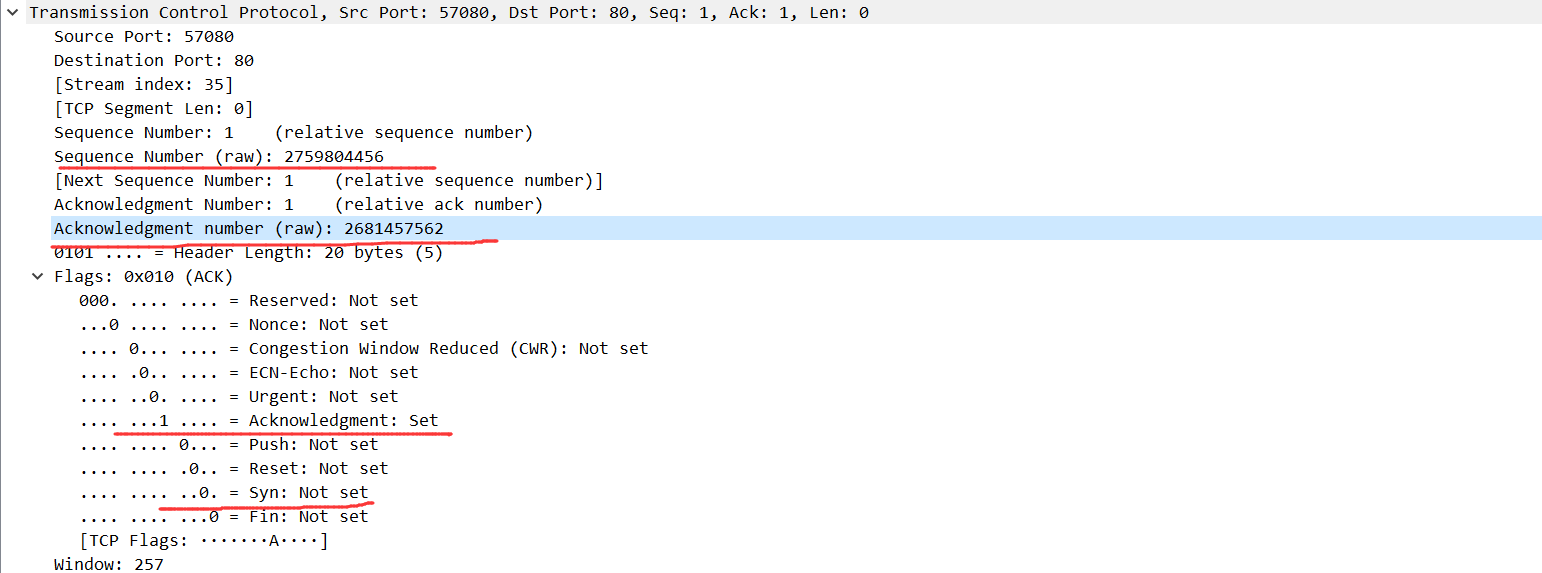
最后，第三次握手的信息如图2.5.5所示，可以看出，ACK=1，SYN=0，序列号seq=0xa47f4628（十进制2759804456），确认号ack=0x9fd3cb9a（十进制2681457562）。序列号与第一次相比+1，确认号等于对方的序列号+1。

图2.5.5 第三次握手

至此，TCP连接建立的三次握手已经完成。

（3）拓扑结构探测实验

1. 主机所在实验室拓扑结构测试

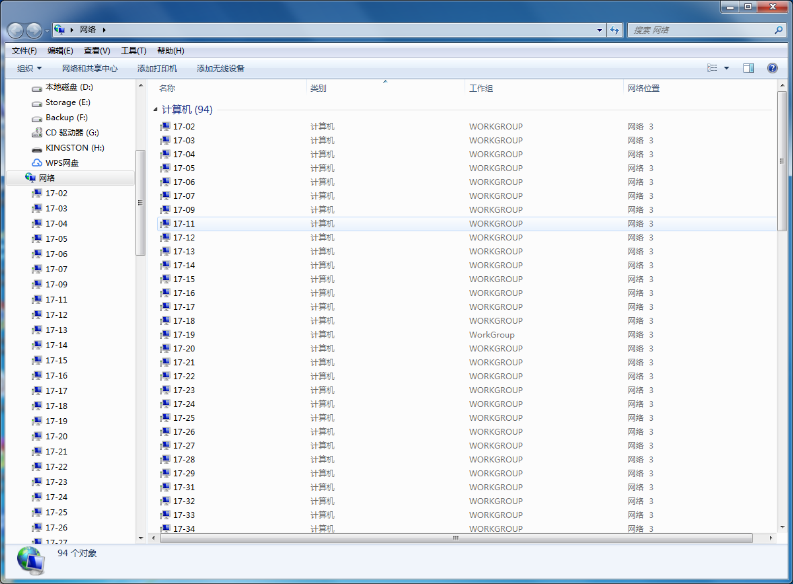
进入计算机桌面，在资源管理器的“网络”中可以看到处在同一个网络内的相邻的主机数以及主机名。如图3.1所示。

图3.1 网络目录树

可以得出结论，该局域网中共有109台主机。

进入cmd，使用tracert命令，探测到达任一相邻主机的中间节点。结果如图3.2所示：

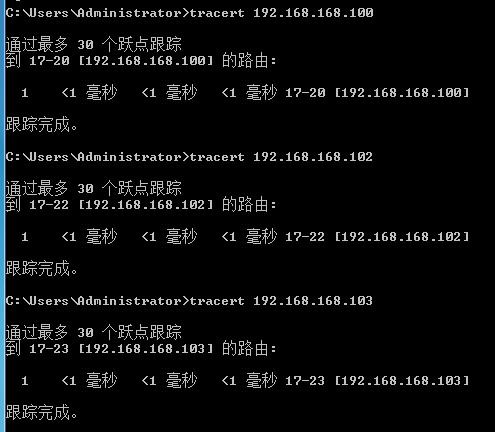
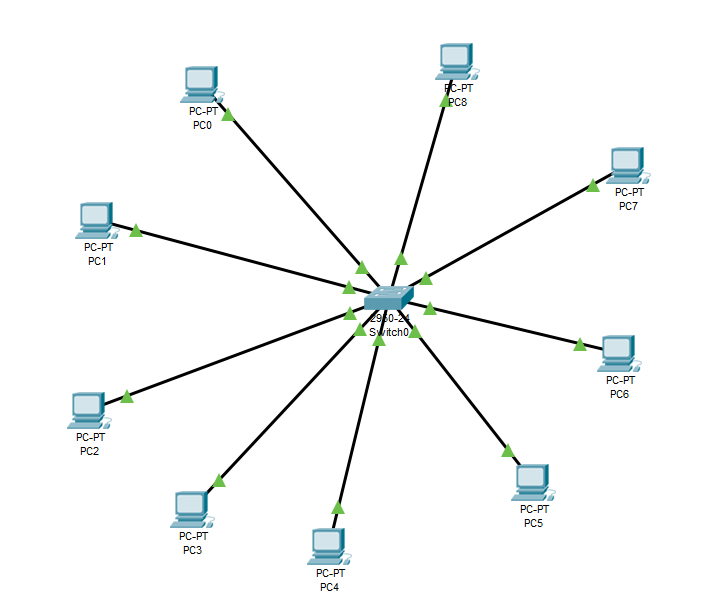
最终发现，到达任一相邻主机的中间节点数均为1。于是可以得到下图所示的实验用机机房的局域网拓扑结构。如图3.3所示：

图3.3 实验室机房的局域网拓扑结构

图3.2 使用tracert追踪相邻的三个主机

1. 所在主机接入校园网路径测试

进入cmd，使用tracert命令，探测访问校园网Web服务器、DNS服务器的路径。结果如图3.4所示：

从探测结果可以看出，本机到达两个不同的服务器的路径存在共同部分，这一段共同路径即为本机接入校园网的路径。

图3.4 探测本机访问校园网Web与DNS服务器的路径

上述测试得到的本机接入校园网的路径为：

本机🡪未知节点🡪192.168.253.1（计算机学院楼网关）🡪172.35.1.2（校园网服务器接入路由器）🡪未知节点🡪服务器(WEB或者DNS)

（4）测试互联网接入路径实验

使用tracert命令测试本机到百度服务器路径，两次测试结果如图4.1、图4.2所示：

图4.1 本机到百度的路径：第一次测试

得到结论：本机接入百度服务器的路径为：

图4.2 本机到百度的路径：第二次测试

本机🡪未知节点🡪192.168.253.1🡪192.168.200.19🡪58.218.185.1🡪222.187.2.213🡪未知节点🡪221.229.234.69🡪202.97.102.154🡪未知节点🡪未知节点🡪106.38.244.150🡪未知节点🡪未知节点🡪未知节点🡪220.101.38.148（百度服务器）

再次追踪，得到新的接入百度服务器的路径为：

本机🡪未知节点🡪192.168.253.1🡪192.168.200.19🡪58.218.185.1🡪222.187.2.213🡪

未知节点🡪221.229.234.69🡪202.97.102.154🡪36.110.245.22🡪未知节点🡪106.38.244.22🡪未知节点🡪106.38.244.150🡪未知节点🡪未知节点🡪未知节点🡪220.181.38.148（百度服务器）

再次使用tracert命令，测试本机到CNN服务器的路径，测试结果如图4.3所示：

图4.3 本机到CNN的路径

得到结论：本机到CNN服务器的路径：

本机🡪未知节点🡪192.168.253.1🡪192.168.200.19🡪153.36.1.121🡪221.6.208.201🡪

221.6.209.197🡪112.85.230.25🡪219.158.116.113🡪219.158.5.146🡪219.158.3.146🡪

129.250.8.93🡪129.250.3.34🡪129.250.6.127🡪117.103.177.74🡪151.101.73.67（CNN服务器）

分析上述对不同服务器的跟踪访问所经历的路径不一样，和对同一服务器的两次访问跟踪所经历的路径不一样，从一样的地方我们得到如下信息：

1. 对百度服务器两次跟踪访问，以及对CNN的访问，三次路径不同，但路径的前若干节点相同，这些节点构成了本机接入互联网的路径。路径如下：

本机🡪未知节点🡪192.168.253.1🡪192.168.200.19🡪互联网

1. 仅分析对百度服务器的两次访问，发现两次不同路径的前若干相同节点更多了，序列如下：

本机🡪未知节点🡪192.168.253.1🡪192.168.200.19🡪58.218.185.1🡪

222.187.2.213🡪未知节点🡪221.229.234.69🡪202.97.102.154

即本机访问百度服务器时，除了离开校园网以外，可能会进入更大的局域网中，从更大的局域网进入互联网。

从不一样的地方我们得到这样的信息：

1. 对百度服务器的两次访问，后面的若干节点不同，说明从校园网到互联网再到百度服务器的路径不同，有可能经过不同的路由器到达。

**实验体会：**

通过本次实验，我深入的理解了计算机网络的层次结构，理解了数据链路层、网络层、运输层以及应用层的数据包的结构。对数据在不同主机之间的流向、传输过程有了更深刻的理解。特别是最后的TCP连接建立的三次握手的过程，通过wireshark明白了具体的连接建立的过程，深受启发。